UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/731,509 | 12/07/2000 | Thomas Schaeck | DE919990082 | 1249 |

46369 7590 11/20/2008

HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 COLUMBIA CIRCLE
ALBANY, NY 12203

| EXAMINER | |
|---|---|
| COLIN, CARL G | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2436 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 11/20/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Application Number: 09/731,509
Filing Date: December 07, 2000
Appellant(s): SCHAECK ET AL.

Wayne F. Reinke, Esq.
Registration No. 36,650
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed September 29, 2008 appealing from the Office action mailed on January 29, 2008.

**(1) Real Party in Interest**

A statement identifying by name the real party in interest is contained in the brief.

**(2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**(3) Status of Claims**

The statement of the status of claims contained in the brief is correct.

**(4) Status of Amendments After Final**

The appellant's statement of the status of amendments after final rejection contained in the brief is correct. However, on page 7, lines 2-3, Appellant adds "No claims were amended or canceled", this statement is not correct.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

| | | |
|---|---|---|
| 4,752,678 | RIKUNA | 6-1988 |
| 5,917,168 | NAKAMURA ET AL | 6-1999 |
| 6,473,500 | RISAFI ET AL | 10-2002 |

**(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

9.1 **Claims 16-20, 22, 25, 28-36, 38-43, and 45-47** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 4,752,678 to **Rikuna** in view of US Patent 5,917,168 to **Nakamura et al**.

As per claim 16, **Rikuna** substantially discloses a method for controlling card holder verification comprising: determining/checking presence of a trusted association between the terminal 12 and the card 11 by comparing a first identifier (i.e. PAN primary account number) stored in card 21 by the comparison section 63 with identifiers (decrypted PAN) stored in terminal 12 (see column 8, lines 5-27) that meets the recitation of *checking the presence of a trusted association between at least one device and a card usable with the at least one device, wherein the checking comprises comparing by one of the card and the at least one device a first identifier stored on the card with one or more identifiers stored in the at least one device a first identifier stored on the card with one or more identifiers stored in the at least one device*. **Rikuna** discloses when the first identifiers coincide (i.e. card is valid), performing cardholder verification separate from the comparing above (see column 8, lines 24-30) that meets the recitation of (*if the checking indicates the presence of the trusted association then performing card holder verification separate from the comparing);* **Rikuna** further discloses cardholder verification is performed separate from the first comparing above by comparing the PIN using the card (comparison section 40) and without a holder of the card providing the PIN (the holder of the card hands in the card for verification) the PIN is provided from the terminal 12 to the card and for comparing by the card to the PIN stored in the card that is different from the PAN (first identifier) (see column 8, lines 38-45 and column

8, lines 58-65, and column 3, lines 9-12) that meets the recitation of *performing card holder verification separate from the comparing using the card and without a holder of the card providing information by providing another identifier to the card from the at least one device for comparing by the card to a second identifier stored on the card that is different from the first identifier*; **Rikuna** also discloses if there is indication that an identifier is not transferred to the terminal (which could be interpreted as no trusted association) then involving the cardholder in performing cardholder verification by directly key inputs the PIN data by the card as in step B15 (see column 9, lines 26-37 and column 8, lines 38-45) that meets the recitation of *otherwise, then involving the holder of the card in performing card holder verification by the card.* **Rikuna** suggests different scenarios in verifying the holder of the card by the card when authentication fails (see column 9, lines 25-67) but is silent about performing the verification when *the checking indicates no trusted association* (i.e. card invalid). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rikuna** to add the feedback mechanism disclosed by **Rikuna** of verifying the cardholder in case of any authentication failure due to the card, the terminal, and the account itself (including trusted association) for the predictable result of ensuring that the holder of the card is authentic as suggested by **Rikuna**

.

**Nakamura et al** in an analogous art discloses automatic debit operation without PIN entry (see column 5, line 39 through column 6, line 7) and further discloses another option is to require PIN entry only when the amount of the transaction exceeds a preselected floor limit to prevent use of a fraudulent issued card to complete a transaction and use of unauthorized terminal (see column 6, lines 11-24) that meets the recitation of *if the checking indicates no trusted association then involving the holder of the card in performing card holder verification by the card.* **Nakamura et al** adds a mutual authentication then would prevent use of a fraudulent issued card and use of unauthorized terminal (see column 6, lines 11-24). Therefore, it would have been

obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rikuna** to involve the holder of the card in performing card holder verification if the checking indicates no trusted association because one of ordinary skill in the art would have recognized the advantages that doing so would prevent use of a fraudulent issued card to complete a transaction and use of unauthorized terminal as suggested by **Nakamura et al**.

As per claim 17, the references as combined above disclose the claimed method of claim 16. **Rikuna** discloses wherein the at least one device is located in a trusted environment (see column 3, lines 15-23).

As per claim 18, the references as combined above disclose the claimed method of claim 16. **Rikuna** discloses wherein the card comprises a chipcard (see column 1, lines 25-30).

As per claim 19, the references as combined above disclose the claimed method of claim 16. **Rikuna** discloses wherein the performing card holder verification without a holder of the card providing information comprises performing card holder verification hidden from the holder of the card (see column 8, lines 38-45 and column 8, lines 58-65).

As per claim 20, the references as combined above disclose the claimed method of claim 19. **Rikuna** discloses wherein the performing card holder verification hidden from the holder of the card comprises automatically obtaining a personal identification number of the holder of the card and verifying the personal identification number without the holder of the card providing the personal identification number (see column 8, lines 38-45 and column 8, lines 58-65).

As per claim 22, the references as combined above disclose the claimed method of claim 16. **Rikuna** discloses wherein the comparing comprises comparing a card identifier stored on the card with one or more card identifiers stored in the device (see column 8, lines 5-27).

As per claim 25, the references as combined above disclose the claimed method of claim 16. **Rikuna** discloses a card storing attribute data including account number, merchant identification code and terminal identification code (device identifier) (see column 4, lines 21-26) and disclose an exemplary embodiment for checking some of the attribute data such as account number, merchant identification code (see column 7, line 40 through column 9, line 23). **Rikuna** is silent about checking terminal identification code meaning comparing an identifier of the device with one or more device identifiers stored on the card. However, it would only require routine skill in the art and design choice to reproduce the process disclosed by **Rikuna** of comparing the other attribute data or identifiers such as account number, merchant identification code, PIN, etc. and use it to compare the terminal identification code (device identifier). One of ordinary skill in the art would have recognized the advantage of comparing terminal identification code so as to determine if the IC card terminal is authorized or not as suggested by **Rikuna** (see column 1, lines 34-36) and as suggested by **Nakamura et al** who discloses mutual authentication for preventing use of unauthorized terminal (see column 6, lines 11-24).

As per claim 28, the references as combined above disclose the claimed method of claim 16, **Rikuna** discloses wherein the performing card holder verification without a holder of the card providing information comprises automatically obtaining a personal identification number of the holder of the card and verifying the personal identification number without requesting information from the holder of the card (see column 8, lines

5-27, column 8, lines 58-65, and column 3, lines 9-12) and wherein the involving the holder of the card comprises requesting the holder of the card to enter the personal identification number (see column 3, lines 21-31).

As per claim 29, the references as combined above disclose further comprising associating the at least one device and the card (see **Rikuna,** column 3, lines 15-23 and column 7, lines 40-52).

As per claim 30, the references as combined above disclose further comprising controlling the association between a device of the at least one device and the card (see **Rikuna,** column 3, lines 15-23 and column 7, lines 40-52).

As per claim 31, the references as combined above disclose wherein the controlling comprises using a network connectable to the device (see **Nakamura et al**, column 5, lines 40-52).

As per claim 32, the references as combined above disclose the claimed method of claim 16, wherein the checking is between at least one device and a plurality of cards and where in the performing card holder verification without a holder of the card providing information is for a plurality of holders (see **Rikuna,** column 2, line 65 through column 3, line 12).

As per claim 33, **Rikuna** substantially discloses a method for performing card holder verification said method comprising: determining/checking presence of a trusted association between the terminal 12 and the card 11 by comparing a first identifier (i.e. PAN primary account number) stored in card 21 by the comparison

section 63 with identifiers (decrypted PAN) stored in terminal 12 (see column 8, lines 5-27) that meets the recitation of *checking the presence of a trusted association between at least one device and a card usable with the at least one device, wherein the checking comprises comparing by one of the card and the at least one device a first identifier stored on the card with one or more identifiers stored in the at least one device a first identifier stored on the card with one or more identifiers stored in the at least one device*. **Rikuna** discloses when the first identifiers coincide (i.e. card is valid), performing cardholder verification separate from the comparing above (see column 8, lines 24-30) that meets the recitation of *performing card holder verification by the card separate from and based on the checking.* **Rikuna** further discloses cardholder verification is performed separate from the first comparing above by comparing the PIN using the card (comparison section 40) and without a holder of the card providing the PIN (the holder of the card hands in the card for verification) the PIN is provided from the terminal 12 to the card and for comparing by the card to the PIN stored in the card that is different from the PAN (first identifier) (see column 8, lines 38-45 and column 8, lines 58-65, and column 3, lines 9-12) that meets the recitation of *if the checking indicates the presence of the trusted association, then a personal identification number of the holder of the card different from the first identifier is automatically provided to the card from the at least one device and verified using the card without the holder of the card providing information*; **Rikuna** also discloses if there is indication that an identifier is not transferred to the terminal (which could be interpreted as no trusted association) then involving the cardholder in performing cardholder verification by directly key inputs the PIN data by the card as in step B15 (see column 9, lines 26-37 and column 8, lines 38-45) that meets the recitation of *otherwise, then the holder of the card is requested to enter the personal identification number to verify the holder of the card via the card comparing the personal identification numbered entered to a second identifier stored on the card*. **Rikuna** suggests different scenarios in verifying the holder of the card by the card when authentication fails (see column 9, lines 25-67)

but is silent about performing the verification when *the checking indicates no trusted association* (i.e. card invalid). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rikuna** to add the feedback mechanism disclosed by **Rikuna** of verifying the cardholder in case of any authentication failure due to the card, the terminal, and the account itself (including trusted association) for the predictable result of ensuring that the holder of the card is authentic as suggested by **Rikuna**.

**Nakamura et al** in an analogous art discloses automatic debit operation without PIN entry (see column 5, line 39 through column 6, line 7) and further discloses another option is to require PIN entry only when the amount of the transaction exceeds a preselected floor limit to prevent use of a fraudulent issued card to complete a transaction and use of unauthorized terminal (see column 6, lines 11-24) that meets the recitation of *if the checking indicates no trusted association then involving the holder of the card in performing card holder verification by the card*. **Nakamura et al** adds a mutual authentication then would prevent use of a fraudulent issued card and use of unauthorized terminal (see column 6, lines 11-24). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rikuna** to involve the holder of the card in performing card holder verification if the checking indicates no trusted association because one of ordinary skill in the art would have recognized the advantages that doing so would prevent use of a fraudulent issued card to complete a transaction and use of unauthorized terminal as suggested by **Nakamura et al**.

As per claim 34, **Rikuna** substantially discloses a system for performing card holder verification said system comprising: determining/checking presence of a trusted association between the terminal 12 and the card 11 by comparing a first identifier (i.e. PAN primary account number) stored in card 21 by the comparison

section 63 with identifiers (decrypted PAN) stored in terminal 12 (see column 8, lines 5-27) that meets the recitation of *means for checking the presence of a trusted association between at least one device and a card usable with the at least one device, wherein the means for checking comprises means for comparing by one of the card and the at least one device a first identifier stored on the card with one or more identifiers stored in the at least one device a first identifier stored on the card with one or more identifiers stored in the at least one device*. **Rikuna** discloses when the first identifiers coincide (i.e. card is valid), performing cardholder verification separate from the comparing above (see column 8, lines 24-30) that meets the recitation of *means for performing card holder verification separate from the comparing using the card.* **Rikuna** further discloses cardholder verification is performed separate from the first comparing above by comparing the PIN using the card (comparison section 40) and without a holder of the card providing the PIN (the holder of the card hands in the card for verification) the PIN is provided from the terminal 12 to the card and for comparing by the card to the PIN stored in the card that is different from the PAN (first identifier) (see column 8, lines 38-45 and column 8, lines 58-65) that meets the recitation of *means for performing card holder verification separate from the comparing using the card and without a holder of the card providing information by providing another identifier to the card from the at least one device for comparing by the card to a second identifier stored on the card that is different from the first identifier if the checking indicates the presence of the trusted association*; **Rikuna** also discloses if there is indication that an identifier is not transferred to the terminal (which could be interpreted as no trusted association) then involving the cardholder in performing cardholder verification by directly key inputs the PIN data by the card as in step B15 (see column 9, lines 26-37 and column 8, lines 38-45, and column 3, lines 9-12) that meets the recitation of *otherwise, then means for involving the holder of the card in performing card holder verification by the card*. **Rikuna** suggests different scenarios in verifying the holder of the card by the card when authentication fails (see column 9, lines 25-67) but is silent about

performing the verification when *the checking indicates no trusted association* (i.e. card invalid). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rikuna** to add the feedback mechanism disclosed by **Rikuna** of verifying the cardholder in case of any authentication failure due to the card, the terminal, and the account itself (including trusted association) for the predictable result of ensuring that the holder of the card is authentic as suggested by **Rikuna**.

**Nakamura et al** in an analogous art discloses automatic debit operation without PIN entry (see column 5, line 39 through column 6, line 7) and further discloses another option is to require PIN entry only when the amount of the transaction exceeds a preselected floor limit to prevent use of a fraudulent issued card to complete a transaction and use of unauthorized terminal (see column 6, lines 11-24) that meets the recitation of *if the checking indicates no trusted association then involving the holder of the card in performing card holder verification by the card.* **Nakamura et al** adds a mutual authentication then would prevent use of a fraudulent issued card and use of unauthorized terminal (see column 6, lines 11-24). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rikuna** to involve the holder of the card in performing card holder verification if the checking indicates no trusted association because one of ordinary skill in the art would have recognized the advantages that doing so would prevent use of a fraudulent issued card to complete a transaction and use of unauthorized terminal as suggested by **Nakamura et al**.

As per claim 35, the references as combined above disclose the claimed system of claim 34, **Rikuna** discloses wherein the means for performing card holder verification without a holder of the card providing information involvement comprises means for performing card holder verification hidden from the holder of the card (see column 8, lines 38-45).

As per claim 36, the references as combined above disclose the claimed system of claim 35, wherein the means for performing card holder verification hidden from the holder of the card comprises means for automatically obtaining a personal identification number of the holder of the card and verifying the personal identification number without the holder of the card providing the personal identification number (see **Rikuna,** column 8, lines 38-45).

As per claim 38, **Rikuna** discloses the claimed system of claim 34, wherein the means for comparing comprises means for comparing a card identifier stored on the card with one or more card identifiers stored in the device (see **Rikuna,** column 8, lines 5-27).

As per claim 39, **Rikuna** discloses the claimed system of claim 34, wherein the means for comparing comprises (comparison section 40) that meets the recitation of means for comparing an identifier of the device with one or more device identifiers stored on the card (see column 2, lines 55-65 and column 3, lines 10-16).

As per claim 40, **Rikuna** substantially discloses a system of performing card holder verification, said system comprising at least one processor (see figure 3) to perform card holder verification based on determining/checking presence of a trusted association between the terminal 12 and the card 11 by comparing a first identifier (i.e. PAN primary account number) stored in card 21 by the comparison section 63 with identifiers (decrypted PAN) tored in terminal 12 (see column 8, lines 5-27) that meets the recitation of *at least one processor on the card to perform card holder verification based on whether a trusted association exists between at least one device and a card usable with the at least one device, and to compare a first identifier*

*stored on the card with one or more identifiers stored in the at least one device.* **Rikuna** discloses when the first identifiers coincide (i.e. card valid) performing cardholder verification separate from the comparing above (see column 8, lines 24-30) that meets the recitation of (*if the checking indicates the presence of the trusted association then performing card holder verification separate from the comparing);* **Rikuna** further discloses cardholder verification is performed separate from the first comparing above by comparing the PIN using the card (comparison section 40) and without a holder of the card providing the PIN (the holder of the card hands in the card for verification) the PIN is provided from the terminal 12 to the card and for comparing by the card to the PIN stored in the card that is different from the PAN (first identifier) (see column 8, lines 38-45 and column 8, lines 58-65, and column 3, lines 9-12) that meets the recitation of *if the checking indicates the presence of the trusted association, then a personal identification number of the holder of the card different from the first identifier of the holder of the card is automatically provided to the card from the at least one device and verified separate from the compare using the card without the holder of the card providing information*; **Rikuna** also discloses if there is indication that an identifier is not transferred to the terminal (which could be interpreted as no trusted association) then involving the cardholder in performing cardholder verification by directly key inputs the PIN data by the card as in step B15 (see column 9, lines 26-37 and column 8, lines 38-45) that meets the recitation of *otherwise, then the holder of the card is requested to enter the personal identification number to verify the holder of the card via the card comparing the personal identification numbered entered to a second identifier stored on the card.* **Rikuna** suggests different scenarios in verifying the holder of the card by the card when authentication fails (see column 9, lines 25-67) but is silent about performing the verification when *the checking indicates no trusted association* (i.e. card invalid). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rikuna** to add the feedback mechanism disclosed by **Rikuna** of verifying the cardholder in case of any authentication failure due to the card, the

terminal, and the account itself (including trusted association) for the predictable result of ensuring that the holder of the card is authentic as suggested by **Rikuna**.

**Nakamura et al** in an analogous art discloses automatic debit operation without PIN entry (see column 5, line 39 through column 6, line 7) and further discloses another option is to require PIN entry only when the amount of the transaction exceeds a preselected floor limit to prevent use of a fraudulent issued card to complete a transaction and use of unauthorized terminal (see column 6, lines 11-24) that meets the recitation of *if the checking indicates no trusted association then involving the holder of the card in performing card holder verification by the card*. **Nakamura et al** adds a mutual authentication then would prevent use of a fraudulent issued card and use of unauthorized terminal (see column 6, lines 11-24). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rikuna** to involve the holder of the card in performing card holder verification if the checking indicates no trusted association because one of ordinary skill in the art would have recognized the advantages that doing so would prevent use of a fraudulent issued card to complete a transaction and use of unauthorized terminal as suggested by **Nakamura et al**.

As per claim 41, **Rikuna** discloses a method to control card holder verification that can be implemented in hardware and software that meets the recitation of an article of manufacture comprising at least one computer usable medium having computer readable program code logic to control card holder verification. Claim 41 recites similar limitations as claim 16 except for incorporating the claimed method into a computer program. Therefore, claim 41 is rejected on the same rationale as the rejection of claim 16.

As per claims 42, 43, 45, and 46,these claims recite the same limitations as claims 19, 20, 22, and 25 respectively except for incorporating the claimed method into a computer program. Therefore, these claims are rejected on the same rationale as the rejection of claims 19, 20, 22, and 25.

As per claim 47, **Rikuna** discloses a method to control card holder verification that can be implemented in hardware and software that meets the recitation of an article of manufacture comprising at least one computer usable medium having computer readable program code logic to control card holder verification. Claim 47 recites similar limitations as claim 33 except for incorporating the claimed method into a computer program. Therefore, claim 47 is rejected on the same rationale as the rejection of claim 33.

9.2 **Claims 23-24 and 26-27** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 4,752,678 to **Rikuna** in view of US Patent 5,917,168 to **Nakamura et al** as applied to claims 16, 22, and 25 and further in view of US Patent 6,473,500 to **Risafi et al.**

As per claim 23, both references disclose the claimed method of claims 16 and 22. **Rikuna** does not explicitly disclose replacing the personal identification number which is a common practice in the art. **Risafi et al** in an analogous art discloses wherein the card identifier is associated with a personal identification number usable in card holder verification and said method further comprises replacing the personal identification number with another personal identification number (see column 4, lines 17-47). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to allow the cardholder to select and change the PIN at any time as taught by **Risafi et al** because it would be advantageous to have the user select a PIN that is easily remembered (see column 3, lines 35-44).

As per claim 24, the references as combined above disclose the claimed method of claim 22, wherein the card identifier is associated with a personal identification number usable in card holder verification, and said method further comprising erasing the association between the card identifier and the personal identification number (see **Risafi et al,** column 4, lines 17-47). Therefore, this claim is rejected on the same rationale as the rejection of claim 23 above.

As per claim 26, the references as combined above disclose the claimed method of claim 25, wherein the device identifier is associated with a personal identification number usable in card holder verification, (see **Rikuna** column 4, lines 21-27) and said method further comprises replacing the personal identification number with another personal identification number (see **Risafi et al,** column 4, lines 17-47). Therefore, this claim is rejected on the same rationale as the rejection of claim 23 above.

As per claim 27, the references as combined above disclose the claimed method of claim 25, wherein the device identifier is associated with a personal identification number usable in card holder verification (see **Rikuna** column 4, lines 21-27), and said method further comprising erasing the association between the card identifier and the personal identification (see **Risafi et al,** column 4, lines 17-47). Therefore, this claim is rejected on the same rationale as the rejection of claim 23 above.

**(10) Response to Argument**

Appellant's arguments pages 10-16 in the appeal brief filed on 9/29/2008 with respect to the claims are not persuasive. With respect to appellant's statement that claims 16-20, 22, 25, 28-36, 38-43 and 45-47 stand

rejected under 35 U.S.C. §103 as allegedly obvious over Rikuna in view of Nakamura. Note that claims 34-47 are cancelled by Appellant and they are not presented for appeal as indicated on Appellant's page 7 brief.

**Regarding claim 16**, Appellant argues (pages 10-11 of appeal brief),

"*both the PAN and EN PAN are stored on and come from the first card. The only thing coming from the terminal is the key for decrypting the EN-PAN, which is not the thing being compared to the PAN. Thus, to clarify, Appellants submit that what was argued was that Rikuna does not disclose that one of the identifiers comes from the terminal, rather than the card*" .

The claim recites,

*comparing by one of the card and the at least one device* ***a first identifier stored on the card*** *with* ***one or more identifiers stored in the at least one device***

It appears that Appellant is arguing where the identifiers come from rather than the claimed language as claimed. Examiner asserts that Rikuna discloses at least two identifiers being compared: the terminal received a first identifier (i.e. PAN primary account number) which was stored on the card memory 35 and compared by the comparison section 63 with identifier (**decrypted PAN**) stored in latch 62 of the terminal 12 (see column 8, lines 5-27). See also column 8, lines 5-23 reproduced below, which states:

"In step B12, first, the primary account number "PAN" and encrypted primary account number "EN-PAN" stored in PAN memory 35 and encrypted PAN memor 36 in user's card 11 are transmitted to the card terminal 12 through interface 42 (see FIG. 3). Then, terminal 12 receives the PAN and EN-PAN data transmitted from card 11 and transmits the PAN data to PAN/MID latch 58 and transmits the EN-PAN data to decryptor 60 through EN-PAN/EN-MID latch 59. Decryptor 60 decrypts the encrypted primary account number EN-PAN on the basis of the key code for decryption to be stored into decryption key code memory 61, thereby allowing it as (PAN) to be latched into decrypted PAN/MID latch 62. **Thereafter,** comparison section 63 compares and collates the primary account number PAN to be latched into PAN/MID latch 58 with the decrypted primary account number (PAN) to be latched into decrypted PAN/MID latch 62

(29) When the PAN transmitted from user's card 11 coincides with the (PAN) decrypted by card terminal 12, the card connected at present is determined to be the valid card issued legally."

Therefore, as disclosed by Rikuna, the decryptor 60 of the terminal performs decryption to generate a decrypted PAN, which is stored in the latch 62 of the terminal before being compared by comparison section 63 with the PAN that was stored in PAN memory 35 in the user's card (see figure 5). Thus Rikana meets the claim recitation of *comparing by one of the card and the at least one device* ***a first identifier stored on the card*** *with* ***one or more identifiers stored in the at least one device.***

Appellant argues on page 12,

*"With regard to the performing aspect of claim 16, the Response to Arguments does not dispute that the Rikuna PIN is always entered into the second card by the card holder before inserting into the terminal. Rather, the final Office Action apparently interprets claim 16 as tying the lack of user input information to the time of performing card holder verification. However, Appellants submit that the claim does not tie the lack of user input information to the time of verification, but only ties that lack of card holder information to the verification process. The fact remains that Rikuna performs a verification process that always includes looking at a PIN that is always entered by the card holder. Thus, Rikuna cannot teach or suggest performing card holder verification without a holder of the card providing information."*

The claim recites

***performing card holder verification*** *separate from the comparing using the card and* ***without a holder of the card providing information by providing another identifier to the card from the at least one device*** *for comparing by the card to a second identifier stored on the card that is different from the first identifier;*

It appears that Appellant is arguing about a difference between the time of verification and what appellant calls verification process. According to the claim language, the time of verification and the verification process is the same because the claim describe the performing of card holder verification with the steps of comparing using the card; providing another identifier to the card from the at least one device without the holder of the card providing information, and the step of comparing by the card. Examiner respectfully disagrees with Appellant's argument as Rikuna discloses in column 2, lines 3-8, that the object of the invention is to not allow the user to be present to directly key-input his PIN during the card holder verification.

"An object of the invention is therefore to provide an IC card system which **can eliminate the necessity** of the cardholder having to visit the card terminal **to directly key-input** his personal identification information even in, for example, restaurants, gas stations, or the like as well". (See column 2, lines 3-8);

Thus a user can record his PIN to be stored in the remote PIN card of a restaurant a long time before the verification takes place (i.e. information may be entered while eating and verification takes place after eating) eliminating the need to directly input information when performing verification as Rikuna discloses,

"for instance, the cardholder calculates an amount of payment on the basis of bill 82 by use of remote PIN entry card 21 during the eating or after completion of the eating. **In step A3**, the cardholder inputs the calculated total amount of payment AMT by operating AMT key 19 of second IC card 21 and also enters his personal identification number "PIN" by operating PIN entry key 18 of second IC card 21, thereby allowing the PIN to be stored into data RAM 29. Thereafter, the cardholder inserts his own user's card (first card) 11 and remote PIN entry card 21 which have already stored both PIN and AMT data, into first and second cardkeepers 83A and 83B of card binder 81 in FIG. 8, respectively, and then puts card binder 81 on the table."

(See column 6, lines 2-16).

Then Rikuna further discloses (see column 6, lines 16-19 and column 8, lines 34-45) the card is picked up by the waitress (within any time period after step A3) **to perform verification**. As interpreted by the Examiner, the verification is performed after the waitress goes to the terminal and inserts both cards into the card terminal, which is when the comparing using the card take place, without asking the holder of the card to provide information by providing another identifier from the at least one device for comparing of the another identifier obtained from the terminal by the card to a second identifier take place. Therefore, card holder verification is performed without a holder of the card providing information by providing another identifier to the card from the at least one device (terminal) as Rikuna discloses:

"The waitress then brings this card binder 81 from the table to a cash register and inserts remote PIN entry card 21 held in binder 81 into card inlet 15 of card terminal 12 (**step A4**)." (see column 6, lines 2-19).

"Thus, the card collating processes in step A7 in FIG. 6 are finished and cardholder collating processes as shown in step A8 will be executed… when it is decided that the PIN which was key input into remote PIN entry card (second card) 21 **in step A3** in FIG. 6 has already been transferred to and stored into terminal 12 in step B9, step B14 follows. The key input PIN data to be stored in terminal 12 is transferred to user's card 11 and latched into PIN latch 34 (see FIG. 3). The key input PIN data latched in PIN latch 34 is collated and compared with the personal identification number (PIN) of the true cardholder or owner of user's card 11 which is preliminarily stored into PIN memory 39 by comparison section 40 in step B15." (see column 8, lines 27-30, 34-45).

"Thereafter, the waitress returns user's card 11 to the cardholder. Namely, since the PIN data which was key input by the cardholder is transferred to card terminal 12 by us of remote PIN entry card 21 which has been preliminarily installed in the store, the cardholder doesn't need to purposely visit the cash register and key input the PIN data but it is sufficient to hand his own user's card (first card) 11 and remote PIN entry card (second card) 21 into which the PIN data was key input to the waitress. Therefore, the deterioration of the atmosphere due to the walk

about of the customer in the store can be prevented. In addition, since the key entry operation of the PIN data by the cardholder is executed at the table, the personal identification number will not be stolen by other persons during the key input operation. Further, since a total amount of payment can be also preliminarily calculated and stored into remote PIN entry card 21, when the card transaction processes are executed, the cash register doesn't need to key input an amount of the bill to the customer." (See column 8, line 57 through column 9, line 8).

Rikuna has disclosed that verification can be performed with the cards and the terminal using only previously stored information in the cards and the terminal without key input during verification. Neither the terminal transferring the PIN nor the user's card performing the comparing asks for the user's PIN to be entered when performing the card holder verification.

Appellant further argues,

*"Finally, against the aspect of claim 16 of involving the holder of the of the card in performing card holder verification if the checking indicates no trusted association, the Response to Arguments cites to Nakamura at column 5, line 64 through column 6, line 16. It is alleged that Nakamura teaches in one embodiment eliminating a PIN and assuming the user is proper, and in another embodiment requiring a PIN only when the transaction amount exceeds a preselected floor. However, in either case, if the Nakamura terminal and card do not authenticate, the result is non-use of the card (see Nakamura at column 6, line 16), rather than card holder involvement in card holder verification."*

Appellant's argument is not persuasive as it appears that Appellant is seeking other result, than what is disclosed by Nakamura by referring only to line 16 in column 6. Nakamura et al discloses automatic debit operation without PIN entry (see column 5, line 39 through column 6, line 7) and further discloses another option is to require PIN entry only (*involving the holder of the card in performing card holder verification by the card* ) when the amount of the transaction exceeds a preselected floor limit (*if the checking indicates no trusted association)* (see column 6, lines 11-24) that meets the recitation of *if the checking indicates no trusted association then involving the holder of the card in performing card holder verification by the card.*

It is noted that in response to Appellant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Therefore, the rejection with respect to claim 16 should be sustained.

**With respect to claim 33**, Appellant submits (see page 13 of Brief) that the remarks made with respect to claim 16 are equally applicable to claim 33. Therefore, the rejection with respect to claim 33 should be sustained in view of the response to arguments made in claim 16 above. Appellant further argues on page 13 that any comparing is done in Rikuna by the terminal. Examiner respectfully disagrees as Rikuna discloses PIN comparison done in the card (see column 9, lines 10-14).

See also column 9, lines 25-37 and column 8, lines 34-45:

"On the other hand, if NO in step B13 in FIG. 7B, namely, when it is determined in ste A3 in FIG. 6 that the PIN data is not key input into remote PIN entry card 21 by the cardholder but user's card 11 has directly been connected to card terminal 12 from the beginning, step B16 follows and the cardholder directly key inputs the PIN data into card terminal 12 (see FIG. 1). Then, **step B15 follows** and if the key input PIN data coincides with the true PIN which has been previously stored, step A9 follows in FIG. 6 similarly to the above and predetermined card processes will be executed." (column 9, lines 25-37).

"when it is decided that the PIN which was key input into remote PIN entry card (second card) 21 in step A3 in FIG. 6 has already been transferred to and stored into terminal 12 in step B9, step B14 follows. The key input PIN data to be stored in terminal 12 is transferred to user's card 11 and latched into PIN latch 34 (see FIG. 3). The key input PIN data latched in PIN latch 34 is collated and **compared** with the personal identification number (PIN) of the true cardholder or owner of user's card 11 which is preliminarily stored into PIN memory 39 by **comparison section 40 in step B15**." (see column 8, lines 34-45).

Therefore, the rejection with respect to claim 33 should be sustained.

**With respect to claim 20**, appellant argues (see pages 13-14) that a PIN in Rikuna is always input by the card holder and therefore cannot meet the claim recitation. However, as mentioned with respect to claim 16 above, the **performing card holder verification** hidden from the holder of the card takes place by automatically obtaining a PIN stored into the terminal by the card without the holder of the card being present for providing the personal identification number (PIN) as claimed in claim 20. The verification is hidden from the holder and any other persons from stealing user's PIN as the holder of the card does not provide information during the verifying because the terminal provides the personal identification number to the user's card hidden from the user and does not ask the user for entering his personal identification number (PIN). Rikuna has disclosed that verification can be performed with the cards and the terminal using only previously stored information in the cards and the terminal without key input during verification as Rikuna discloses,

"The waitress then brings this card binder 81 from the table to a cash register and inserts remote PIN entry card 21 held in binder 81 into card inlet 15 of card terminal 12 (**step A4**)." (see column 6, lines 2-19).

"Thus, the card collating processes in step A7 in FIG. 6 are finished and cardholder collating processes as shown in step A8 will be executed... when it is decided that the PIN which was key input into remote PIN entry card (second card) 21 **in step A3** in FIG. 6 has already been transferred to and stored into terminal 12 in step B9, step B14 follows. The key input PIN data to be stored in terminal 12 is transferred to user's card 11 and latched into PIN latch 34 (see FIG. 3). The key input PIN data latched in PIN latch 34 is collated and compared with the personal identification number (PIN) of the true cardholder or owner of user's card 11 which is preliminarily stored into PIN memory 39 by comparison section 40 in step B15." (see column 8, lines 27-30, 34-45).

"Thereafter, the waitress returns user's card 11 to the cardholder. Namely, since the PIN data which was key input by the cardholder is transferred to card terminal 12 by us of remote PIN entry card 21 which

has been preliminarily installed in the store, the cardholder doesn't need to purposely visit the cash register and key input the PIN data but it is sufficient to hand his own user's card (first card) 11 and remote PIN entry card (second card) 21 into which the PIN data was key input to the waitress. Therefore, the deterioration of the atmosphere due to the walk about of the customer in the store can be prevented. In addition, since the key entry operation of the PIN data by the cardholder is executed at the table, the personal identification number will not be stolen by other persons during the key input operation. Further, since a total amount of payment can be also preliminarily calculated and stored into remote PIN entry card 21, when the card transaction processes are executed, the cash register doesn't need to key input an amount of the bill to the customer." (See column 8, line 57 through column 9, line 8).

Therefore, the rejection with respect to claim 20 should be sustained.

**Regarding claim 29,** Appellant argues, (see page 14) that Rikuna fails to teach creating an association between the user's card and the terminal. Examiner respectfully disagrees and asserts that Rikuna discloses the claim limitation "***associating the at least one device and the card***" as Rikuna states,

"Various kinds of data such as a total amount of a billing "AMT" and the like including, e.g., merchant identification code "MID" for every store to which first card 11 was registered and terminal identification code "TID" for every terminal are stored into data memory 41." (See column 4, lines 22-27).

In step B4, card terminal 12 transmits the card terminal attribute data indicative of the kind of this terminal to user's card 11. Card 11 receives this card terminal attribute data and checks to see whether this kind is adaptable to the card terminal or not. On the other hand, in step B5, user's card 11 also transmits the card attribute data, stored in ROM 33, indicative of the kind of this card to card terminal 12. Terminal 12

receives this card attribute data and checks to see whether this kind is adaptable to the card terminal or not. (See column 7, lines 56-67).

Therefore, the rejection with respect to claim 29 should be sustained.

**Regarding claim 30,** Appellant argues, (see pages 14-15) that Rikuna fails to teach controlling the association between the user's card and the terminal. Examiner respectfully disagrees and asserts that Rikuna discloses the claim limitation "***controlling the at least one device and the card***" as Rikuna states,

"Various kinds of data such as a total amount of a billing "AMT" and the like including, e.g., merchant identification code "MID" for every store to which first card 11 was registered and terminal identification code "TID" for every terminal are stored into data memory 41." (See column 4, lines 22-27).

In step B4, card terminal 12 transmits the card terminal attribute data indicative of the kind of this terminal to user's card 11. Card 11 receives this card terminal attribute data and checks to see whether this kind is adaptable to the card terminal or not. On the other hand, in step B5, user's card 11 also transmits the card attribute data, stored in ROM 33, indicative of the kind of this card to card terminal 12. Terminal 12 receives this card attribute data and checks to see whether this kind is adaptable to the card terminal or not. (See column 7, lines 56-67).

Therefore, the rejection with respect to claim 30 should be sustained.

**Claims 17-19, 22, 25, 28, and 31-32** are not separately argued by Appellant and therefore, the rejection with respect to these claims should be sustained.

**With respect to claim 24**, Appellant argues that Risafi does not disclose erasing the association between a card identifier and the PIN because appellant states "erasing the association, for example still allows the same PIN." Examiner respectfully disagrees as Risafi discloses allowing a cardholder to change the PIN number associated with the card identifier at any time (see column 12, lines 20-38 and column 4, lines 17-47), which meets the claimed recitation "erasing the association". In response to Appellant's argument that the references fail to show certain features of Appellant's invention, it is noted that the features upon which Appellant relies (i.e., erasing the association, for example still allows the same PIN) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

**With respect to claim 27**, Appellant submits (see page 16 of Brief) that the remarks made with respect to claim 24 are equally applicable to claim 27. Therefore, the rejection with respect to claim 27 should be sustained in view of the response to arguments made in claim 24 above.

**Claims 23 and 26** are not separately argued by Appellant and therefore, the rejection with respect to these claims should be sustained.

**(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Carl Colin/
Primary Examiner, Art Unit 2436
November 10, 2008

Conferees:

Nasser Moazzami

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435

INTERNATIONAL BUSINESS MACHINES CORPORATION
NEW ORCHARD ROAD
ARMONK, NEW YORK 10504